How We Lead with Trust:

Cisco's Code of Business Conduct

Welcome message from Chuck Robbins, Chair and CEO

Team,

One of Cisco's core differentiators is the trust we've built with both internal and external stakeholders. This trust is an integral part of who we are at Cisco, and we earn and protect it every day, with every interaction. Bringing ethics and integrity into all that we do is a shared responsibility and it's up to each of us to take ownership and accountability for always doing the right thing.

Our Code of Business Conduct (Code) outlines the principles we abide by and the intentionally high standards to which we hold ourselves. We use it to guide our daily actions and decisions – in how we develop products and services, engage with customers, interact with our partners and suppliers, or support other areas of our business. Our Code is just the starting point though.

Applying our Code and following Cisco's policies will help each of us manage the risks that are inherent in our roles and ultimately help drive our overall collective success. Thank you for your commitment to the principles and standards outlined in our Code and your ongoing focus to protect and preserve the trust we've built together.

Chuck Robbins
Chair and CEO

Table of Contents

We Know Our Code and Speak Up

Every person at Cisco has an opportunity to lead the way to innovation and excellence. We do this by being trustworthy, responsible, and accountable.

Our Code is a helpful guide to acting with trust within our business and with others. It applies to all Cisco employees, directors, and executive officers, and to all Cisco subsidiaries and affiliates. Read and use our Code when you have questions.

Being trustworthy and accountable doesn't mean always having the answers, but it does mean taking steps to find them. As your first stop when a decision is unclear, review our Code and the guidance linked in it. If you need help or have questions, ask your manager, ask any Cisco leader, your P&C, Finance, or Legal support. Ask questions whenever you are unsure — email the **Ethics & Compliance Team** for advice. We are all expected to exercise good judgment and act responsibly.

We all have a responsibility to speak up when something doesn't feel right — even if we don't have all of the details. If you see or suspect a violation of our Code or Cisco policy, speak up. You can report concerns anonymously where permitted by law to the **Cisco EthicsLine**. Your report will be handled promptly, efficiently, and with every effort to maintain confidentiality.

Reporting Options

You have options when reporting concerns. Choose the option you are most comfortable using.

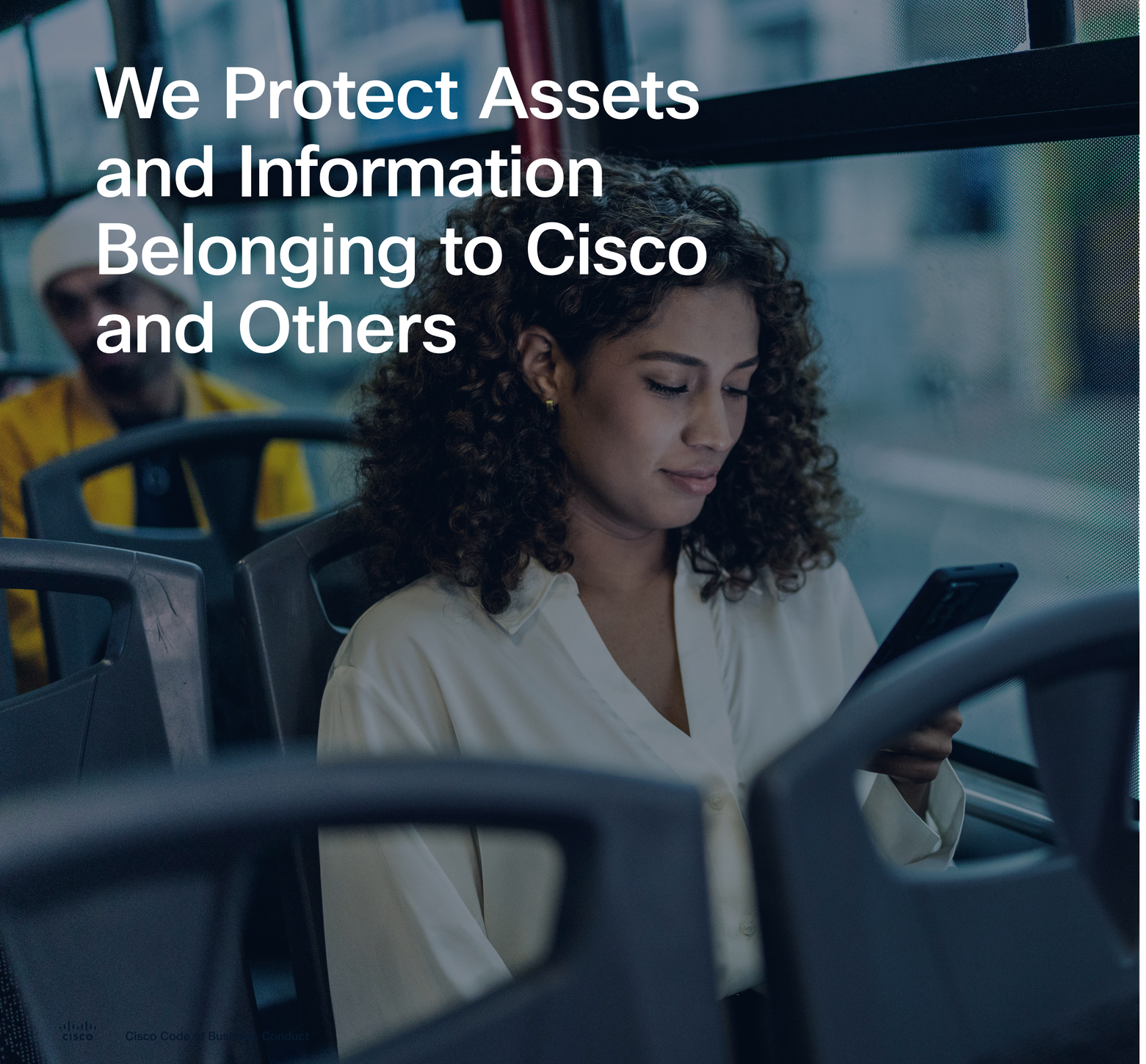
- **Cisco EthicsLine** (available by webform or phone, 24 hours x 7 days per week in 27 languages)
- Your Manager
- Your People & Communities Representative
- Your Legal or Finance Team
- **The Ethics & Compliance Team**
- **Threat.Cisco.com** for known or suspected cybersecurity incidents and data incidents
- **Corporate Security Centers** for physical safety and security concerns
- **Global Employee Relations** for personal and workplace concerns

No Retaliation

At Cisco, we value open and transparent communication, and we are committed to handling your concerns with care. Cisco supports those who raise genuine concerns, even if they turn out to be mistaken. Retaliation and threats of retaliation are strictly prohibited. Retaliating against someone who asks a question, raises a genuine concern, or participates in an investigation is itself a violation of our Code.

Lead The Way

People leaders model trust and accountability every day. As a leader, you are responsible for creating an environment where people feel safe to speak up, ask questions, and raise concerns without fear of retaliation. Never pressure employees to achieve results in ways that violate our Code, Cisco's policies, or the law. Promptly report concerns using the **Cisco EthicsLine** or the reporting option you are most comfortable using.



We Protect Assets and Information Belonging to Cisco and Others

Cisco's assets are vital to our business and long-term success. We must safeguard and use them properly – this includes physical spaces, devices, software, intellectual property, and data. Likewise, when handling others' assets or information, we must protect them and use them only as authorized and for their intended purpose. Respecting ownership rights preserves the trust of our customers, partners, and suppliers.

Safeguard Physical Assets

Handle Information and Data Responsibly

Use Technology Responsibly and Securely

Preserve and Respect Intellectual Property Rights

Safeguard Physical Assets

We are all responsible for safeguarding Cisco's physical property – from workspaces and facilities to computers, devices, equipment, and supplies. Cisco's assets are for business use and should be treated with care.

Trust Means:

- Protecting assets from theft, damage, waste, and misuse. This includes securing devices when not in use.
- Not borrowing or removing Cisco assets from Cisco facilities without proper authorization.

Consider This

Cisco assets are for business purposes and should be used responsibly, securely, and consistent with Cisco's policies. Use of Cisco's assets is not private. To protect company property and resources, Cisco may monitor any assets and devices used to conduct business.

Learn More

- Use of Cisco Assets Policy
- Use of Cisco Premises Policy

Use Technology Responsibly and Securely

Networks, platforms, software, and other technology are essential to how we work – but misuse or mistakes can lead to cybercrime, unauthorized data access or exposure, loss of confidential information, reputational damage, regulatory action, or lawsuits. Incidents can happen in an instant so it's important to stay alert, and follow all Cisco policies related to security, privacy, and the use of AI.

Trust Means:

- Creating strong passwords, safeguarding login credentials, and using multi-factor authentication.
- Connecting to a Cisco network or VPN when accessing confidential information and not attempting to disable or circumvent network controls.
- Verifying website addresses and being vigilant against phishing and other social engineering attacks.
- Only downloading approved software and keeping devices and applications updated.
- Not accessing, distributing, downloading, or uploading illegal or inappropriate material.

Learn More

- Acceptable Use Policy
- Trusted Device Standard
- Keep Cisco Safe

Handle Information and Data Responsibly

Information and data are also valuable assets and how we handle them is critical to maintaining trust in Cisco. Much of the information we encounter in doing our jobs is proprietary to Cisco and must be protected. Confidential information – whether from Cisco, customers, partners, or others – requires additional care. We are all responsible for preventing data losses or breaches, and for never accessing, using, or sharing information improperly.

Trust Means:

- Following Cisco's **data classification** and handling policies.
- Collecting, accessing, and sharing proprietary, confidential, and third-party information only as authorized and for a valid business purpose.
- Using AI responsibly – only using approved AI tools and only with the level of data classification permitted for each specific tool.
- Handling personal data with sensitivity and transparency, fairness, and accountability; observing special requirements when handling sensitive personal data, like protected health information and other regulated data.
- Preventing improper disclosure of confidential and proprietary information by not displaying or discussing it where you might be seen or overheard by others.
- Immediately reporting suspected compromise of confidential information to **Threat.Cisco.com**.

Learn More

Data Protection Policy
Privacy Center of Excellence - Policies and Standards
Data Protection Standard
Data Classification & Taxonomy
AI Governance

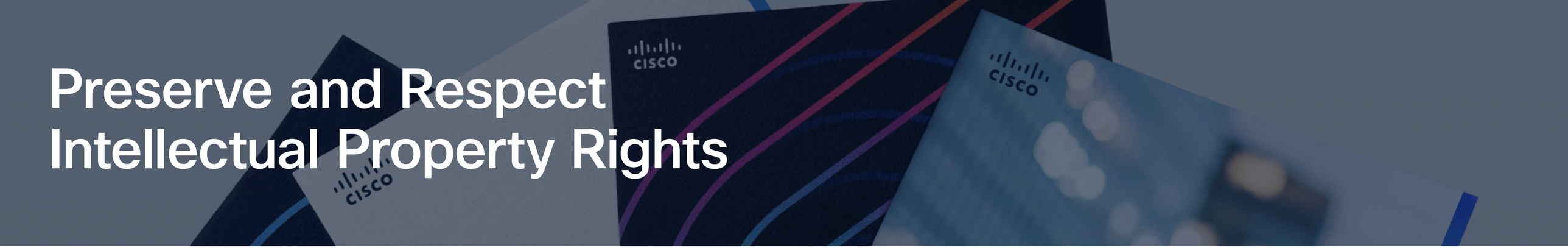
Consider This

Nearly all information owned or generated by Cisco is proprietary including:

- Business plans, projections, or company developments
- Earnings, unannounced results, and other financial data
- Management communications
- Everyday business information on our systems and networks
- Software, code, and other innovations and creative works, such as handbooks, brand assets, and website material

Personal Data (or **Personally Identifiable Information (PII)**) is any information that can reasonably be used to identify an individual or otherwise make an individual identifiable, and may include name, address, email address, phone number, or login credentials.

- **Sensitive Personal Data** is a subset of Personal Data that is either categorized as sensitive under the law, relates to individuals in vulnerable communities, requires breach notification, or has the potential to result in significant harm to the data subject if the data is compromised (including discrimination, identity theft, and physical or financial harms).



Preserve and Respect Intellectual Property Rights

Intellectual property lays the foundation for our products, brand, and business. These assets are critical to Cisco's continued leadership in our industry and they differentiate us with our customers. We protect these assets and respect the intellectual property rights of others. The trust of our customers, partners, and even our competitors depends on preserving intellectual property rights inside and outside of Cisco.

Trust Means:

- Using Cisco's trademarks, copyrighted works, and other intellectual property only for approved business purposes.
- Reporting unethical or unauthorized use of intellectual property, for example, our company logo or source code.
- Recognizing the intellectual property of others; never accessing, distributing, downloading, or uploading it without permission; and not bringing trade secrets from prior employers to Cisco.
- Remembering that anything you improve or create in the course of your job, including technical innovations, belongs to Cisco.
- Promptly disclosing any external development activity, including contributions to open-source projects, even if conducted on your own time.

Learn More

Cisco Intellectual Property Online (CIPOL)

Consider This

Intellectual property is intangible property, such as patents, copyrights, trademarks, and trade secrets. It includes a wide range of things from our source code, manufacturing processes, training materials, and internal technical knowledge.

We Compete Fairly and in Compliance with Laws

We build trust by competing fairly and selling on the quality and value of Cisco's offerings. We compete vigorously, but we do so ethically and lawfully. Remember, playing to win is not just about what we sell, but also how we sell it.

- Promote Competition
- Follow Rules for Doing Business in Public Sector
- Prevent Bribery and Corruption
- Observe Global Trade Requirements

Promote Competition

Cisco encourages competition in the marketplace, which benefits customers and promotes innovation. We prohibit business practices that reduce competition, even unintentionally or indirectly. This applies to how we interact with competitors, work with channel partners, and engage with our customers.

Trust Means:

- Never coordinating actions or sharing competitively sensitive information with competitors, including price, customers, or market details.
- Promoting competition among channel partners by treating them fairly and based on objective criteria, especially when it comes to discounts and customer opportunities.
- Not setting resale prices or margins for channel partners nor fixing pricing with customers who buy through partners.

Learn More

Antitrust Policy
Antitrust Compliance and Training

Prevent Bribery and Corruption

We conduct our business transparently and honestly, and we require the same from our partners and suppliers. We do not tolerate bribery or corruption anywhere in our business.

Trust Means:

- Winning business on merit – never offering, giving, or accepting anything of value to improperly influence a business decision or gain an unfair advantage, avoiding even the appearance of impropriety.
- Only offering or accepting gifts, travel, entertainment or other things of value that have a legitimate business purpose and are reasonable, appropriate, and permitted under applicable laws and policy.
- Identifying Government/ State-Owned Entity (G/SOE) employees and obtaining required approvals before offering anything of value.
- Obtaining pre-approvals and clearly documenting the objective basis for offering non-standard discounts, incentives, and any other discretionary benefits.
- Never allowing a third party to do something on Cisco's behalf that Cisco is not allowed to do itself.
- When engaging suppliers, partners, or other third parties, following onboarding processes, monitoring their activities, and addressing potential concerns quickly.

Learn More

Global Anti-Corruption and Anti-Bribery Policy
Gifts, Travel, and Entertainment (GTE)
U.S. Public Sector Hospitality Guidelines
G/SOE Look Up Tool
Supplier Code of Conduct
Partner Code of Conduct

Consider This

'Anything of value' is more than gifts, meals, travel, lodging, or entertainment. Charitable donations, sponsorships, non-standard discounts, channel incentives, favorable commercial terms, and favors or personal benefits, such as loans, education, jobs (paid or unpaid), or investment opportunities, are all 'things of value.' Anything of value can be considered a bribe if it is given for an improper purpose.

Government officials include anyone who works for a **Government/State-Owned Entity (G/SOE)**, commonly referred to as 'public sector.'

- A full definition of G/SOE is available in the **Gifts, Travel, and Entertainment (GTE) Policy**.
- It's not always clear whether an entity is a G/SOE. Sales segmentation is not a reliable indicator.
- Cisco's definition may differ from how entities are defined by law. So, take the time to review the definition and use Cisco's tools and resources to identify potential G/SOEs before offering anything of value.

Follow Rules for Doing Business in Public Sector

Cisco sells directly and indirectly to government entities (G/SOEs) around the world. These customers have specific public sector and procurement rules that go beyond our standard commercial obligations. As a trusted partner to government customers, we must take steps to proactively identify and comply with all applicable regulations and procedures. Contact Legal for help with questions relating to public sector requirements.

Trust Means:

- Before engaging in U.S. public sector business, reading and understanding our **U.S. Public Sector Ethics Code** which includes additional obligations.
- Not drafting bid or tender language for a G/SOE if Cisco intends to bid on the contract, and never seeking, accepting, sharing, or using bid information that's not available to all bidders.
- Following public sector procurement rules, including those governing limited-source opportunities and competitive bidding processes.
- Being truthful, complete, and accurate when invoicing and responding to G/SOE bids, certifications, or other information requests.

Learn More

U.S. Public Sector Legal

Observe Global Trade Requirements

Cisco is subject to trade controls – including import, export, sanctions, and antiboycott laws – around the world. Trade regulations impact the flow of Cisco hardware, software, technology, information, and services between countries. Violations can lead to significant penalties and harm our ability to do business. Trade controls are fast-moving and complex, so it's important to know the requirements and seek assistance when needed.

Trust Means:

- Not conducting business in or with embargoed regions: Cuba, Iran, North Korea, or the Crimea, Donetsk, and Luhansk regions of Ukraine.
- Providing complete and accurate data – such as product classifications, country of origin, government authorizations, and valuation – with order and shipping requests.
- Initiating **Export Product Reviews** for all new offerings.
- Coordinating with Global Trade Legal & Compliance before responding to antiboycott requests or hiring citizens of embargoed regions.

Learn More

Global Trade Legal & Compliance (TLC) Site
Global Export Policy
Global Internal Shipping Compliance Policy
Acceptable Use Policy

We Are Accurate, Honest, and Complete

Building trust means committing to accuracy, honesty, and transparency in everything we do. We're responsible for keeping and reporting accurate information and properly retaining business records. We follow all internal controls, processes, and policies to preserve our company's financial integrity and operational efficiency. By holding ourselves to these standards, we protect Cisco and maintain our reputation as an ethical business.

Document and Report Information Accurately

Obtain Necessary Approvals and Adhere to Internal Controls

Follow Record Retention Requirements

Document and Report Information Accurately

Cisco relies on employees to provide accurate, complete, and honest information. Whether you're submitting expense reports, recording time worked, or providing sales data, it's essential that we get this right. Maintaining accurate books and records is essential to Cisco's strategy and meeting our reporting obligations.

Trust Means:

- Providing accurate, complete, and objective information in all communications, and avoiding misrepresentations or misleading others.
- Recording all income and expenses promptly, including when paying vendors, submitting expenses, and booking deals.
- Not mischaracterizing transactions or creating off-book or "parked" funds.
- Cooperating fully with company requests for information in investigations, audits, and other reviews.

Employees with financial reporting responsibilities
Cisco's CEO, CFO, and all Finance department employees are also bound by the Financial Officer Code of Ethics which includes additional obligations to ensure fair and timely reporting of Cisco's financial results and condition.

Consider This

- **Off-Book or "parked" funds** are funds placed in a non-Cisco account where the use of the funds is directed by Cisco employees without proper transparency, authorization, or documentation. They are a violation of policy even if ultimately used for legitimate business purposes. Examples include using unspent budget to prepay a vendor for work in future quarters, or giving a partner extra discounts to offset customer travel or compensate for a past deal.
- Company decisions and investor trust depend on each of us providing accurate information. When you are unsure what information to provide, which processes to follow, or whose approval you need, ask for help. If mistakes happen or relevant information is left out, reach out and correct it. Remember, an omission itself may be a misrepresentation or may mislead others.

Learn More

Global Expense Policy
Financial Officer Code of Ethics

Obtain Necessary Approvals and Adhere to Internal Controls

Securing approvals and following internal processes helps Cisco receive the best value, record expenses and income accurately, and avoid unauthorized commitments. This builds trust with our internal and external stakeholders, ensures Cisco's funds are spent wisely, and supports our obligations as a public company.

Trust Means:

- Obtaining required approvals and following internal processes before buying goods and services, incurring expenses, or offering non-standard terms.
- Not circumventing a required process or encouraging others to do so – deadlines or pressure from a colleague, manager or customer are not an excuse.
- Ensuring written agreements clearly reflect the actual terms of the deal and never making side commitments.
- Notifying Finance immediately of any order booked before an end customer has issued a valid purchase order to Cisco or our channel partner (known as a 'soft booking').

Learn More

[Global Bookings Policy]
[Non-Standard Deal Policy]
[Global Procurement Services]

Consider This

- Discounts can be essential to meet a competitor's price or a customer's budget, but misused discounts can erode profits, fund corruption, compromise the accuracy of Cisco's records, and facilitate product diversion. Approve or request discounts only with a clear business case and document and account for them properly.
- A **side commitment** or **"side letter"** is any unauthorized commitment or representation, verbal or written, to a customer, partner, or other third party that is made outside of Cisco's contracting and approval processes. Sharing deal pricing prior to approval, agreeing to accept returns outside of a contract, or promising future incentives or concessions are examples of side commitments and are prohibited.

Follow Record and Retention Requirements

Creating, maintaining, and disposing of business records is part of our daily work. Practicing good records management helps us run our business smoothly and efficiently, protect records appropriately, and satisfy our obligations to others.

Trust Means:

- Creating, identifying, and categorizing business records properly, which may include emails, instant messages, documents, collaboration tools, or electronic files.
- Retaining, managing, and disposing of records in accordance with Cisco's records retention policies and Legal directives.

Learn More

Enterprise Data Retention and Destruction Policy
Email Retention and Proper Use Policy
Instant Messaging Policy

We Separate Personal and Business Interests

Doing our jobs means doing what's right for Cisco. Although our personal and professional lives are often separate, they sometimes overlap. When they do, we are responsible for protecting Cisco's interests and maintaining the trust of our colleagues, customers and partners.

- Manage Conflicts of Interest
- Prevent Insider Trading
- Exercise Care When Speaking Publicly
- Separate Personal Political Involvement

Manage Conflicts of Interest

A conflict of interest occurs when our personal activities or relationships interfere, or appear to interfere, with Cisco's best interests. Conflicts can affect objectivity and credibility and get in the way of doing what's right for the company. We must take proactive steps to disclose, document and seek help to resolve conflicts that arise. Even the appearance of a conflict can damage trust in Cisco and employees.

Trust Means:

- Avoiding or withdrawing from activities or relationships that may influence or appear to influence Cisco's business or your job responsibilities.
- Using Cisco processes to promptly disclose potential conflicts, even if you are unsure if a conflict exists or you believe your decision-making will not be affected; and obtaining approval where required.

Learn More

[Conflicts of Interest, External Boards and Investments Policy]
[Conflicts of Interest Resources]
[Conflicts of Interest Disclosure Tool]

Consider This

Conflicts of interest can arise in many different situations, such as:

- Work outside of the company, whether paid or unpaid, including as a contractor, consultant, or advisor
- Board participation
- Investments or ownership interests by you or a family member
- Development of outside inventions or intellectual property
- Personal relationships with others at Cisco or within our industry

We must be especially mindful of conflicts when activities or relationships involve partners, suppliers, competitors, public sector entities, or others in Cisco's ecosystem.

Prevent Insider Trading

While working at Cisco, you may learn of material “inside” information about Cisco or another public company that is not available to the public – referred to as material non-public information. Using or disclosing this information for anyone’s personal benefit is unethical, and against the law. Violations can have serious consequences for individuals and companies.

Trust Means:

- Recognizing when you have material non-public information and protecting it from inappropriate disclosure.
- Not trading on insider information or sharing it with others who could trade on it.
- Never trade in Cisco derivatives or hedge Cisco securities.

Learn More [Insider Trading Policy]

Consider This

Material non-public information isn’t just undisclosed financial information – it can relate to nearly any aspect of a company’s business and operations, such as:

- Proposed mergers, acquisitions, or divestitures
- Significant management or personnel changes
- New products or services
- Changes in key business relationships

Reach out to **insidertradingattorney@cisco.com** with any questions.

Exercise Care When Speaking Publicly

External statements have a powerful impact on Cisco's brand and reputation. Cisco must speak with one voice, sharing clear, accurate, and appropriate information, coordinated at the right time.

Trust Means:

- Only speaking on behalf of Cisco when you have authorization to do so and making it clear when your statements are your own
- Getting approval before speaking with media or analysts, committing to an endorsement, being interviewed or participating in a speaking engagement, accepting a vendor award, or publishing a blog or article about Cisco or our business.
- Being respectful and professional online, including on social media.
- Following restrictions on sharing company information and intellectual property when speaking or posting publicly.

Learn More

Social & Digital Media Policy
Endorsement Policy
Speaker Opportunity Policy
Media Spokesperson Policy

Separate Personal Political Involvement

Cisco respects our rights as individuals to actively participate in the political process using our own time and resources. However, all personal political participation must remain separate from Cisco.

Trust Means:

- Not using Cisco assets – including company funds, facilities, equipment, communication channels, or brands – to support political candidates, causes, parties, or organizations.
- Making it clear that personal political views are your own and do not represent Cisco's views.
- Never engaging in lobbying or other political activity on Cisco's behalf unless authorized by Government Affairs.

Learn More

Cisco Government Affairs

We Promote Safe, Respectful Workplaces Inside and Outside of Cisco

Respect guides how we work together and with others. When we treat people with fairness and dignity, contribute to a safe workplace, and honor our environmental obligations, we build trust within Cisco and with our partners and communities.

Practice and Expect Respectful Treatment

Promote Safe Work Environments

Honor Our External Obligations

Practice and Expect Respectful Treatment

Everyone deserves to feel valued and included at work. At Cisco, we build belonging through everyday actions – listening openly, recognizing each other's strengths, and speaking up when something isn't right. We don't tolerate discrimination, harassment, bullying, or retaliation in any form, including actions based on legally protected characteristics. Instead, we contribute to a culture of trust, respect, and fairness, where everyone has an opportunity to succeed.

Trust Means:

- Treating everyone with dignity and making employment decisions based on qualifications and performance, not bias.
- Avoiding jokes, language, or physical contact that could be unwelcome or offensive, even unintentionally.
- Supporting accommodations for individuals with disabilities, helping everyone feel able to do their best work.

Learn More

[Equal Employment Opportunity (EEO) Policy]
[Harassment in the Workplace Policy]
[Reasonable Accommodation Policy]

Consider This

- **Protected characteristics** are traits and attributes protected by law. These include but are not limited to: age, ancestry, color, caste, citizenship, gender, gender expression, gender identity, genetic information, marital status, medical condition, national origin, physical or mental disability, pregnancy, race, religion, sex, sexual orientation, and military or veteran status.
- Our Code applies whether you're in the office, working virtually, at a customer location, or at any work-related event. No matter the environment, respect is built in the small moments, and it's not always obvious when a comment or action crosses the line. Pause and ask yourself: How might my words or actions affect someone else? If you see disrespectful behavior, call it out even when it's uncomfortable.

Promote Safe Work Environments

At Cisco, we are all entitled to a safe, secure, and supportive workplace. We protect ourselves and each other by being aware of our surroundings, following safety protocols, and creating space where everyone can focus and thrive.

Trust Means:

- Following safety and security instructions, policies, and practices.
- Following badge access rules at Cisco facilities and events.
- Recognizing workplace hazards and reporting injuries, accidents, unsafe acts, and unsecure conditions right away. Threats and acts of violence will not be tolerated.

Learn More

Global Access Control Policy
Drugs & Alcohol in the Workplace Policy
Corporate Security Center
Environmental Health & Safety Page

Honor Our External Obligations

Guided by globally recognized standards and following applicable laws, we strive to further human rights and responsible practices across our business.

Trust Means:

- Following our human rights policy, which includes immediately reporting concerns about forced labor or human trafficking in our supply chain or with third parties with whom Cisco does business.
- Following our internal policies focused on reducing environmental impact and making accurate representations about Cisco's products.

Learn More

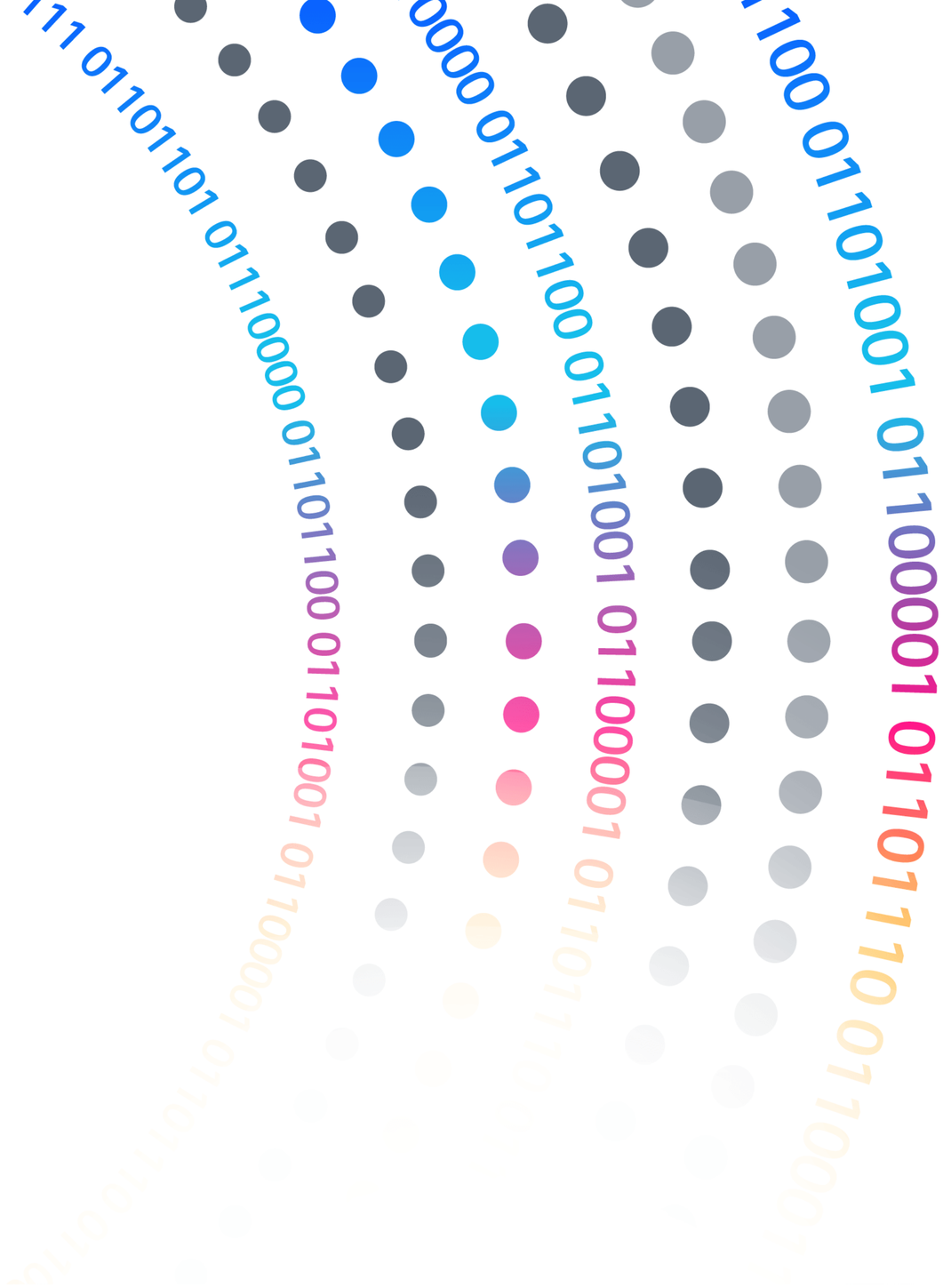
Global Human Rights Policy
Corporate Environmental Policy

Our Responsibilities

Every good and ethical choice you make builds the culture that makes Cisco work. When you lead with trust by following our Code, choosing integrity over convenience, speaking up over silence, and accountability rather than looking the other way, you inspire others to do the same. The trust we've built together is earned through countless daily decisions by people who choose to do what's right, even when it's hard, and when no one is watching.

You are responsible for following our Code, Cisco's policies, and applicable laws. Violating our Code may result in disciplinary action, up to and including termination. If you see something that doesn't seem right, you must speak up.

All Cisco employees are required to complete assigned training on our Code and related policies. Completing this training is essential to meeting your responsibilities and upholding Cisco's standards. When each of us leads with trust and accountability, we create the foundation for the impact we'll achieve together.



Last Revision: February 2026